VOTIRO

GUIDE

Revolutionizing Data Security

Zero Trust Data Detection & Response

New Threats, Same Problems

There's no denying that ensuring the security and privacy of sensitive data is more of a challenge than ever before. Unauthorized disclosures or leaking of this data through cyber-attacks, file sharing, and collaboration (for starters) creates compliance and privacy nightmares.

While the focus has previously been around structured data, much of the problem stems from unstructured data, which makes up 80% of all data in the enterprise. Comprising emails, documents, and general files, unstructured data frequently stores sensitive information and hidden threats and is responsible for 71% of security incidents. Many traditional solutions are simply unequipped to handle data while it's in motion, and in the modern world, there's not much left that isn't moving from one sensitive endpoint to another.

With so much private data scattered throughout an organization, data can be lost in many ways. It can be stolen maliciously through zero-day malware, ransomware, or direct attacks. The loss may even come from inside sources passing it outside the organization via email or cloud storage. Though sometimes, the problem is simply due to negligence, where a user accidentally sends sensitive information to the wrong person, creating an incident that spirals out of IT's controls.

With so many ways to lose data, organizations must ask themselves, how do we secure it all?

Tradition for Tradition's Sake?

Traditional security tools are designed for a more predictable digital environment, such as **antivirus (AV)** and **endpoint detection and response (EDR)**, each struggling to provide effective real-time prevention of sophisticated attacks and data compromises. Many of these tools react only after an incident, merely driving alerts that teams can respond to. However, the attack has already happened, and damage has been done, with data most likely being compromised in the process.

Adding to these challenges, traditional data protection tools like **Data Loss Prevention (DLP)** and even modern **Data Security Posture Management (DSPM)** tools offer visibility but often fail to automate responses, thus offering no preventative measures for private data leakage in the first place. This inadequacy in proactive security measures can come at a steep cost, with data breaches costing organizations an average of $4.45 million per year. The key? Proactive security to help avoid these costs by detecting and remediating the problem before it ever exists.

This guide delves into data security challenges, exploring the need for a proactive and comprehensive approach to safeguard personal identifiable information (PII) and other sensitive content as it flows into and throughout an organization.

It will highlight the necessity of adopting advanced solutions, such as **Zero Trust Data Detection & Response**, that adapt to the unique challenges of unstructured data and evolving cyber threats, ensuring the continuous and secure flow of information vital for business success.

The Evolving Threat Landscape

Cybersecurity has long been a challenge for organizations to keep up with, and it's only getting more complicated with dramatic changes to the threat landscape. Challenges include the rise of generative AI, shadow IT, and a dependency on unstructured data. This evolution presents a challenge for traditional security tools primarily designed for a more predictable and structured digital environment. As it stands, these once-dominant, conventional tools are finding it increasingly difficult to adapt to the dynamic and complex nature of modern cyber threats. Traditional defense mechanisms, once reliable, now struggle to provide effective real-time prevention of attacks and data compromises. Let's dig into the obstacles many IT teams and SOCs face today.

The Risks of Shadow IT and Shadow SaaS

Shadow IT is any technology not deployed and actively maintained by IT. With the proliferation of shadow IT, thanks in part to large tech stacks and an ever-growing need to "set and forget" processes, the cybersecurity landscape has become complicated, to put it lightly. These untracked and unmanaged systems create enormous risks for organizations, creating new attack surfaces not accounted for in an organization's central security strategy. Because they are untracked and unmanaged, they lack patching and security hardening, leaving them open to exploitation. **Attackers actively target these systems** as soft targets, knowing they may contain sensitive data or provide easy access for deeper penetration into the organization's network, often serving as an easy entry point for malware and data exfiltration.

Once-dominant, conventional tools are finding it increasingly difficult to adapt to the dynamic and complex nature of modern cyber threats.

Software as a Dis-Service

Shadow IT systems are rarely created out of malice or incompetence but rather due to the rapid pace of technological advancement and operational demands. These systems might result from temporary solutions or outdated tech that's been overlooked. The original intentions for a timely follow-up or removal of these systems often get sidetracked, leaving them vulnerable to security risks. This oversight can lead to the exposure of private data in ways that are neither secured nor tracked, amplifying the risk of data breaches and unauthorized access. Once an organization has found itself with a Shadow IT problem, identifying and getting up to speed can be a long, uphill battle.

This issue extends beyond just on-premises IT systems, encompassing untracked **Software as a Service (SaaS)** platforms and cloud assets that are built but poorly managed or entirely unmanaged. **Different departments within an organization might independently purchase solutions and forget to inform the IT department, leading to a fragmented IT environment.** These uncoordinated actions can result in sensitive information being stored in insecure locations without proper oversight. This decentralization and lack of communication creates inefficiencies and exposes the organization to heightened cybersecurity risks. According to our 2023 survey of cybersecurity experts, over a third of organizations (36%) lack comprehensive visibility into the channels through which files enter. One-third might seem insignificant until you realize how many vendors and cloud storage enterprises can be compromised alongside a data breach.

Shadow IT also stems from developer actions in the cloud, where devs can easily activate components without central oversight, creating new, often unnoticed, attack surfaces. These rapidly developed and deployed assets, whether proofs of concept or production systems, can lack security patches and maintenance, leaving vulnerabilities unchecked.

“Generative AI is the worst form of shadow IT.”
— Eric Avigdor, Votiro Chief Product Officer

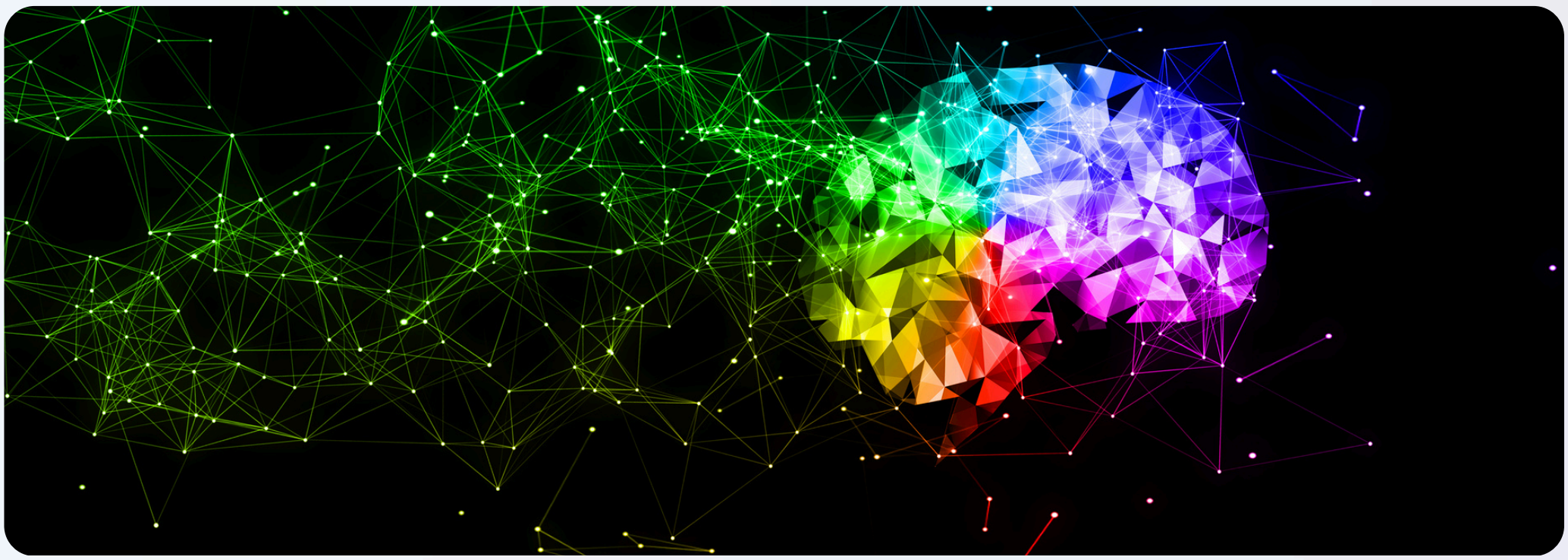
One Step Forward, Another Step Back: **The Growth of Generative AI**

Generative Artificial Intelligence (GenAI) is the use of machine-learning models to train AI to create new data in the form of text, audio, images, and videos. With the release of popular, public-facing programs like ChatGPT, Copilot, Bard, and DALL-E, the quick advancements in GenAI have significantly complicated the cybersecurity landscape by introducing new types of vulnerabilities—not only opening new doorways for threat actors, but via the exposure of private data that’s being ingested alongside an internet’s worth of information.

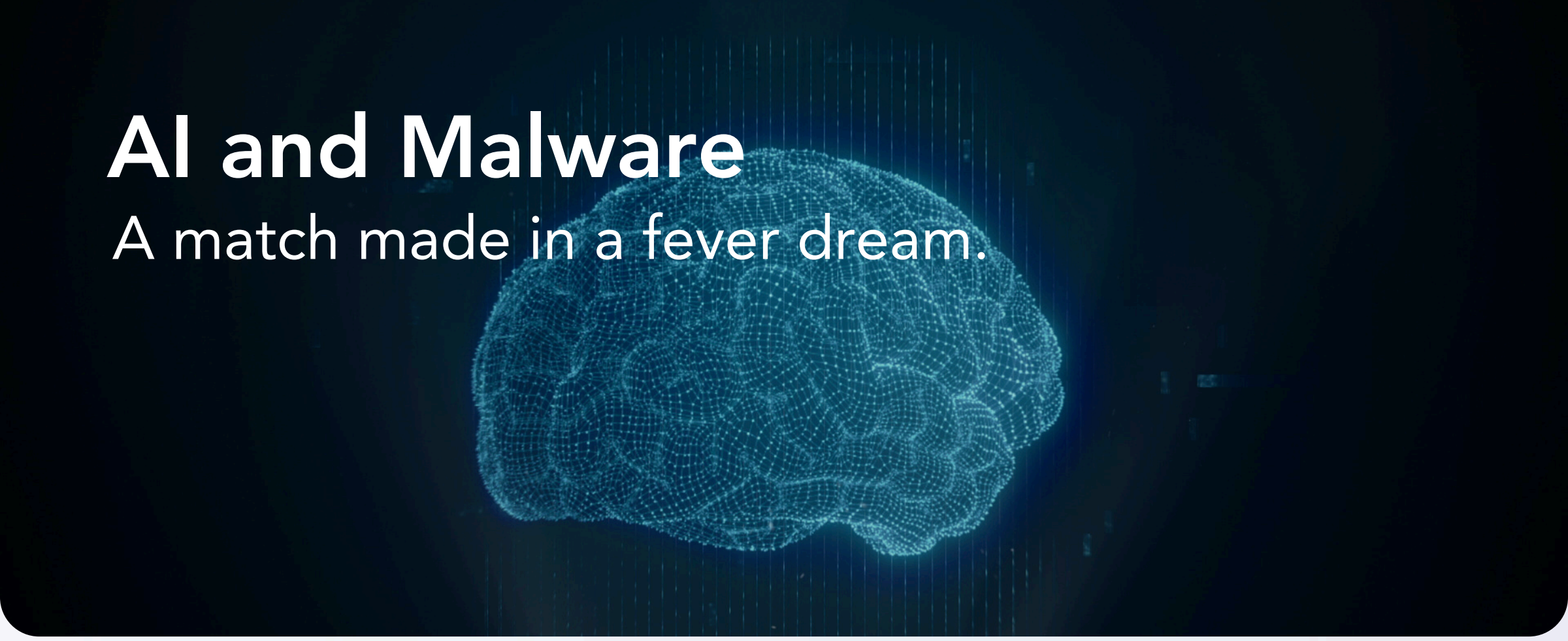
A byproduct of this unregulated data consumption is outgoing data contamination that may contain hidden threats as well as private information not meant for public dissemination.

Many threats leverage the very training data used by AI. By using private data for training models, GenAI has created significant data security challenges and privacy risks. When integrated into AI and **machine learning (ML)** models, private data can significantly enhance these systems' accuracy and functionality. However, this practice raises two critical concerns: the **potential bias in model outputs** and the **risk of private data exposure**.

When private data is used to train AI and ML models, there is an inherent risk of embedding existing biases into the systems. These biases can manifest in several ways, depending on the nature of the data and its original context. For instance, if a dataset predominantly contains information from a particular demographic group, the AI model may perform better for that group than others, leading to skewed or unfair outcomes. This bias can affect decision-making processes in critical areas such as healthcare, employment, and law enforcement, where AI-driven decisions can profoundly impact individuals' lives.



A significant concern for cybersecurity professionals and organizational IT teams is the exposure of private data through its use in AI models, particularly with large language models (LLMs) like GPT (Generative Pre-trained Transformer). LLMs are trained on vast amounts of text data, some of which may include PII, healthcare information, and payment card data. When these models generate text based on their training, they can inadvertently produce outputs that contain echoes of the training data, potentially exposing private information. This exposure poses privacy risks and legal implications, particularly under regulations such as **GDPR (General Data Protection Regulation)**, which mandates strict handling and protection of personal data.



AI and Malware

A match made in a fever dream.

One of the most concerning developments in the proliferation of AI is its use in modifying existing malware, creating unique threats that are more difficult to detect and counter. Traditional cybersecurity tools such as AV are designed to recognize and respond to malware variants using known signatures. When used for harm, **AI is able to take existing malware and modify it so that the signatures are no longer recognized by AV**, preventing prompt recognition and mitigation.

AI further complicates these malware challenges by augmenting phishing, one of the prime delivery vectors for hidden threats. It automates and refines phishing campaigns, allowing them to target users better with more sophisticated and believable language. AI analyzes extensive data sets to craft highly personalized phishing messages that closely mimic legitimate communications, making them harder for users to identify. **This approach helps cybercriminals bypass traditional anti-phishing tools and achieve higher success rates in their campaigns, increasing the spread of malware.**

The threat of AI also extends into traditional cyberattacks, helping cybercriminals amplify the speed and scale of their processes, making it harder for existing defenses to keep up. Automated AI-enabled attacks are rapidly developed, deployed, and executed at scales previously unattainable by human attackers while increasing their complexity and reach. If principles, such as Zero Trust, are not in place, this can quickly overwhelm many existing cybersecurity tools, increasing the likelihood of a breach.

The Unstructured Data Dilemma

Unstructured data, comprising emails, videos, social media posts, and documents, is a foundation of modern business practices. **Unlike structured data, which is easily searchable and can be efficiently scanned for sensitive information, unstructured data presents a more complex scenario.**

False Alarms

Unstructured data sources do not conform to a standard template or structure, making them more prone to false positives and negatives in security monitoring. As any IT professional can attest, false positives and the constant barrage of alarms in need of inspection eat up valuable bandwidth that is better spent on real security threats. In fact, a Morning Consult survey showed that SOCs spend a third of their day dealing with false positives.

Classification

Even with advanced data classification techniques, effectively identifying and protecting sensitive information within unstructured data remains a significant challenge. Its varied formats and the sheer volume in which it is produced only add to the complexity, posing substantial hurdles in management and security. Without proper insights and mitigation, this can lead to severe alert fatigue that compounds upon an already stressed IT environment.

Data in Motion

Cybercriminals target unstructured data because of the valuable information it often contains and how widespread it is throughout an organization. Rather than attacking hardened storage such as databases, unstructured data exists across media, collaboration software, and user systems. Its widespread nature makes it harder to apply traditional security controls, making it easier for attackers to find and steal. This is why organizations must investigate data security solutions that protect unstructured data in-motion.

Attacks, Exposures, and Compliance Nightmares

The Challenges of Modern Data Security Solutions

With a staggering 31% year-over-year increase in cyberattacks, and incidents occurring an astonishing 26,000 times per day (approximately every three seconds), organizations need to adapt and evolve in order to survive the next zero-day attack.

However, these challenges extend beyond new and emerging threats. As much as times are changing in the digital ecosphere, existing hurdles still pose significant problems. Hidden threats embedded within data often go undetected due to the limitations of current detection technologies. These threats can lurk in everyday business operations, unseen and unaddressed until they manifest in harmful ways. Additionally, the data security space is highly fragmented, with a multitude of solutions that often operate in silos. This fragmentation leads to gaps in security, as no single solution tends to provide comprehensive protection. All in all, this makes it harder to meet compliance and privacy requirements while protecting sensitive data.

> In light of cyber risks increasing, cyberthreats proliferating and a changing operating environment, it is more critical than ever for organizations to build and optimize a cybersecurity program. It is the cornerstone of cybersecurity initiatives which help security and risk management leaders secure new environments, protect against the expanded attack surface, consume security capabilities in new ways and create better efficiencies through automation."
>
> — Shailendra Upadhyay, Senior Research Principal at Gartner

Risks Posed by Hidden Threats

According to SC Magazine, one of the first challenges organizations face is the ever-present and growing malware problem, which has nearly doubled from 2022 to 2023. These concealed dangers, particularly in files and data sharing, pose significant risks to organizations, often bypassing traditional security measures.

The cost of ransomware, a common form of such hidden threats, extends beyond direct financial implications, such as paying the ransom, compliance fines, and legal costs. There are also considerable indirect costs, including the time spent to halt an infection, assess its impact, and the resultant non-productivity for all affected parties. This situation is exacerbated by the inadequacy of traditional security tools, which often fail to detect and prevent these sophisticated threats in real time. Then, as is the nature of a malware infection, the theft of private data is soon to follow.

Data Protection and Privacy

Data security encompasses far more than just safeguarding against external threats; it crucially involves the protection and privacy of sensitive information within an organization. A key area of concern is the safeguarding of private data within documents. Despite rigorous security measures, sensitive data is often at risk of being improperly managed or inadvertently transmitted to unauthorized destinations. Such lapses can lead to significant breaches, jeopardizing customer trust and exposing the organization to legal and regulatory consequences.

This has led many organizations to look at Data Detection & Response as a solution to their data security problems. But more on that later...

Data in Motion

In addition to compliance concerns, organizations face the complex challenge of discovering and securing sensitive data while it flows. This involves tracking and protecting data as it traverses different systems and networks, a task made difficult by the sheer volume and velocity of data exchange in modern enterprises through email, collaboration tools, and file sharing.

Ensuring sensitive data is identified and appropriately handled in real-time demands advanced data classification and monitoring capabilities. With the right tools, data masking and anonymization techniques can alter or obscure sensitive information as its discovered, protecting individual privacy while retaining data utility. Failing to classify and protect this data can lead to data breaches and non-compliance, making it crucial that all incoming data is accurately identified in motion and appropriately classified. Yet, **layered tech stacks come with layered problems in the form of manual data classification** – each tool demanding its own classification parameters, and when they don't align with other tools in the stack this can lead to non-compliance even with the best intentions in mind.

Organizations must find a balance in securing sensitive information while maintaining operational efficiency and data accessibility. While a logical starting point, implementing DLP and DSPM solutions alone can bring their own set of technical and business challenges.

- **DLP systems** must constantly evolve to counteract the advanced tactics of cybercriminals and adapt to changing data formats and communication methods. This can put an unnecessary burden on security teams as they try and keep up with an ever-evolving risk surface that requires time to mitigate when Zero Trust is not in play.
- **DSPM tools**, on the other hand, are essential for assessing and enhancing data security posture, yet they too must dynamically adjust to the evolving nature of data environments. This includes addressing compliance requirements, consistently classifying sensitive data, and proactively identifying potential vulnerabilities.

So, what's an organization to do? The key component is in providing context-based data protection and privacy while tailoring policies to the specific needs and risks of different data types and scenarios. A process that demands automation and proactivity, and a balance which requires more than traditional DLP and DSPM solutions alone.

Frag/men/ta/tion
in the Data Security Space

Companies have adopted numerous security solutions to address specific problems in their organization. These tools are optimized for what they do best, but rarely do they integrate efficiently with other solutions. This disconnect has led to fragmentation within tech stacks and has caused integration and management difficulties that lead to security gaps.

Problems include dealing with numerous vendors, licenses, and interfaces, which can escalate costs and add complexity, straining resources and leading to operational inefficiencies. All of this fragmentation hinders effective threat detection and response. When security systems operate in silos, there may be critical gaps in coverage, and a lack of coordinated response can significantly delay threat mitigation efforts.

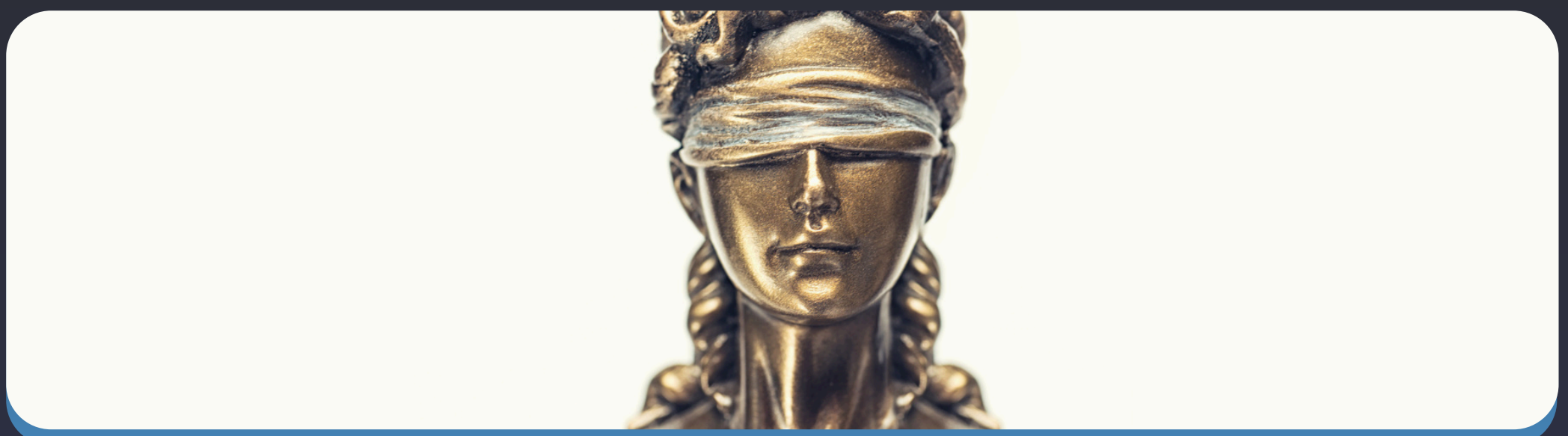
An integrated security approach is the only way to overcome a fragmented landscape.

Unified, holistic solutions offer several benefits over a piecemeal approach. They provide improved threat visibility by consolidating data from various sources, leading to a more accurate and comprehensive understanding of the security landscape. Furthermore, they simplify management and enhance the overall efficacy of security measures meant to prevent cyber threats.

Such a strategy should encompass:

- Real-time privacy and compliance tools to shield sensitive information should unintended access be granted
- Proactive threat prevention, such as **Content Disarm & Reconstruction (CDR)** to thwart novel malware
- Endpoint security should a threat ever make it into your environment
- Network defenses and cloud security to ensure no area is left vulnerable
- Threat analytics to better understand current risks to data, as well as assess critical gaps and prepare for shifts in future attack methodologies

Compliance and Privacy: All in DDR's Wheelhouse



Data security is only the start of data management challenges for organizations. Compliance and data privacy regulations also complicate things, with different countries and regions having their own laws, such as GDPR and Schrems II in the EU, the CCPA (California Consumer Privacy Act), PDPA in Singapore, and Australia's Privacy Act 1988 and APP (Australian Privacy Principles).

These must be followed along with industry-specific rules such as the **Payment Card Industry Data Security Standard (PCI-DSS)** and the more public-facing **Health Insurance Portability and Accountability Act (HIPAA)**, each adding its own regulations and constraints around sensitive data handling.

These rules go beyond how data is stored and secured; they also set rules around what type of data businesses can collect and ensure the amount of data is scoped to a targeted purpose. Meeting these mandates requires organizational rules to manage data collection and track utilization internally and with trusted partners. Doing this may take several security solutions to meet protection standards and prove alignment with each necessary standard.

While we're beginning to sound like a broken record, it must be said that this all leads to the need for an integrated data security solution that takes compliance and the protection of PII, PHI, and PCI-DSS into account, rather than requiring multiple solutions to meet the same goal.

No More Looking Back
Addressing Cybersecurity's Reactive Posture

Many organizations fall victim to taking a reactive cybersecurity posture, waiting for problems to occur before addressing them.

This is partially due to how many of these tools function. Their strategies focus on taking action after a breach or attack has already begun, relying on known signatures to be identified. This leads to a delayed response – days, weeks, even years after the fact – leaving room for incalculable damage in the meantime. Extended response times allow cybercriminals additional time to steal more data, increasing the breach's overall financial and reputational impact. Addressing a breach right away is great, if not ideal, but admitting a gap in your defenses has been sitting open for weeks really points to a lack of consumer protection, and consumers are not likely to forget.

A purely reactive stance also leaves organizations unprepared for emerging threats, as their capabilities rely on detection.

Any detective solution requires seeing a threat before or locating clues from system behavior that may indicate a novel attack. This approach creates additional risk for organizations by increasing the likelihood that a unique, zero-day threat will not be immediately detected, increasing both incident length and impact. To put it simply, it's equivalent to locking your doors after a break-in: they may not come back, but the damage is already done – and a change of address is likely on the horizon.

Addressing a breach right away is great, if not ideal, but admitting a gap in your defenses has been sitting open for weeks really points to a lack of consumer protection, and consumers are not likely to forget.

The Importance of a Proactive Cybersecurity Posture

Proactive cybersecurity prevents attacks before they happen. This approach involves identifying and addressing potential threats and weaknesses early on. Doing so makes it more difficult for cybercriminals to succeed, even with advanced tactics or new vulnerabilities. It can also lead to less reliance on complicated tech stacks and ongoing (i.e., costly) threat management.

By using a proactive strategy, organizations maintain uninterrupted business operations and safeguard their reputation by ensuring that cybersecurity issues don't disrupt day-to-day activities.

It's Zero Trust or Bust

Traditional security models work much like a fortress. They rely on strong perimeter defenses like a firewall, trusting everyone inside the perimeter by default – or at least giving them much less scrutiny.

On the other hand, Zero Trust assumes that nobody inside or outside the network is trusted by default, pushing the controls closer to the data itself rather than relying on the perimeter to do its job. Every time access is requested for a network resource, it must be verified, regardless of the source or how many times it's been allowed in. By adopting this approach, Zero Trust reduces the blast radius from breaches, limiting the damage that can be done by a successful attacker.

In addition to giving IT teams the power to control access and set policies, Zero Trust protection goes even further. It leverages enhanced monitoring and real-time detection to keep an eye on all network traffic rather than just external requests – which most legacy security measures rely on. This actionable approach helps teams rapidly identify and mitigate suspicious activities, reducing the window of opportunity for a breach to occur.

Zero Trust is one of the most effective ways to shift from a reactive mindset to a proactive one.

Supporting Innovation without Sacrificing Security

While proactive security sounds great on paper, there are still obstacles to consider to make it practical.

For instance, cloud adoption has improved business development and growth, allowing teams to rapidly innovate and shift from ideation to production in no time. With cloud technologies, developers can quickly build and deploy applications, sidestepping the traditional, time-consuming, and costly hardware procurement and configuration processes. By leveraging 'Infrastructure as Code' to streamline the assembly and deployment of IT infrastructure, organizations can adapt and scale with little upfront investment.

However, this rapid development and deployment is not without challenges. The speed at which infrastructure is built often surpasses the rate at which its security can be thoroughly assessed and assured. This leads to a scenario where the infrastructure might be ready for use faster than it can be secured, allowing sensitive data to potentially enter insecure environments. In some cases, this sensitive data is part of the intended design. Still, the security controls may fall short of meeting the stringent compliance requirements necessary for the organization.

Cybersecurity in the Age of Oversharing

The widespread use of collaboration tools (e.g., Slack, Teams, OneDrive, box) has enabled teams to work together seamlessly across the globe in real-time, with nearly 80% of workers utilizing collaboration tools for their jobs. This adoption of online collaboration has markedly reshaped work and community engagement strategies across industries. Now here comes the “however...” part.

While this instant sharing of data fosters innovation and efficiency, it also means that any hidden threats within the data are shared just as rapidly. Each file becomes a nexus of collaboration, linking disparate teams and locations. The same pathways that facilitate this seamless collaboration can also become conduits for the rapid spread of malware. Once introduced into the network, a single infected file can swiftly propagate across the organization, bypassing traditional defenses due to the trusted nature of internal sharing. Who here can say they haven’t shared the latest meme in a work chat or downloaded the latest threat report to their company PC without a second thought? We’re certainly not throwing stones.

No Business is an Island

Much of the data that flows into an organization comes from external sources essential for various operational needs. This is particularly evident in the fintech sector, where businesses are often legally required to collect customer documents to verify identity. To compound an already innocuous vulnerability, **even commonly perceived “safe” formats like PDFs, Word documents, and images can be potential vectors for security threats**.

The key to protecting all this innovation lies in implementing robust, agile security measures that can keep pace with the rapid development cycles and instant data sharing. Businesses must ensure that their internal processes, collaboration tools, and cloud infrastructure are not only equipped to facilitate innovation but also secure-by-design to prevent potential vulnerabilities from being exploited – without ever impacting the end-user.

Acronyms Everwhere:

DDR vs CSPM vs DSPM and the Rest

When working to create a secure-by-design infrastructure, three critical methodologies stand out for their unique but complementary capabilities in safeguarding an organization's data and IT infrastructure:

- Data Detection and Response (DDR)
- Cloud Security Posture Management (CSPM)
- Data Security Posture Management (DSPM)

These tools help secure by design, preventing potential vulnerabilities from being exploited and ensuring that an organization's data and IT infrastructure are protected against the vast array of cyber threats that organizations face each and every day. **Now, let's look into their differences...**

DDR starts with a data-centric security approach, emphasizing protecting the data regardless of location through proactive threat identification, advanced analytics, and machine learning techniques to provide real-time detection and threat response. This combination of technologies effectively detects known and unique threats as they occur and automates the response, significantly reducing the time between detection and mitigation and reducing potential damage from cyber incidents. This approach is particularly effective for highly regulated organizations whose sensitive data is a target for cybercriminals.

CSPM, unlike DDR, focuses on cloud environments rather than data security. It specializes in monitoring and managing cloud infrastructures by assessing the environment's security posture to ensure that configurations comply with regulatory standards. They identify risks due to misconfigurations, providing guidance on remediation and allowing teams to modify misconfigurations before attackers can take advantage of them. Despite the focus on management, CSPM still requires IT to take manual steps in order to resolve conflicts, as well as leaving the cloud environment open to threats without the proper tools in place.

DSPM, as the name implies, complements DDR and CSPM by focusing on data security posture management. This approach involves discovering and classifying sensitive data across various environments, a crucial step in managing and protecting critical data assets. DSPM tools monitor who has access to sensitive data and detect abnormal activities, thus safeguarding against insider and external threats. DSPM also excels at policy enforcement and compliance, ensuring that data handling policies are strictly followed and helping maintain compliance with specific data protection laws. However, as is the case with CSPM, DSPM is a good approach for understanding your posture but does not proactively prevent threats that can expose sensitive data, nor does DSPM automate mitigation efforts.

Proactive.
Real-time.
Actionable.

The Shift to Zero Trust Data Detection & Response

Zero Trust Data Detection & Response represents a comprehensive and forward-thinking approach to cybersecurity, tailor-made for addressing the evolving challenges of today's complex threat landscape.

This method embodies a shift towards real-time, proactive threat prevention and data protection, which is necessary in an era where cyber threats are increasingly sophisticated and elusive. By adapting a Zero Trust approach to data security, this level of DDR treats every file and data packet as a potential threat until proven otherwise. This ensures that every element and interaction within the network undergoes rigorous scrutiny and validation – offering protection from both sides of the data security coin: malware threats and privacy risks.

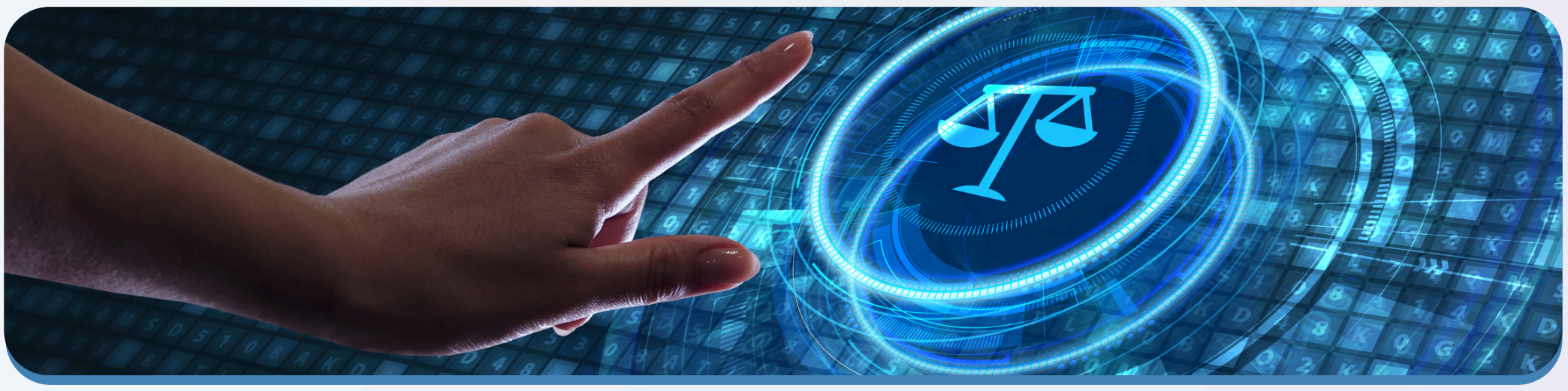
Zero Trust DDR's strength lies in its ability to identify and disarm the hidden threats that lurk within files and shared data – the kind of threats that traditional security measures, such as AV, often miss, and endpoint and posture solutions don't fully address until after the fact. Leveraging advanced Content Disarm & Reconstruction to disarm hidden threats, such as ransomware, at their source, Zero Trust DDR preemptively eliminates potential data exposures down the line.

What Does Zero Trust DDR Mean for Security Posture?

Zero Trust DDR isn't just about combating hidden threats: it's about unifying security threat protection with data privacy capabilities. At its core, Zero Trust DDR is data-driven, rather than identity-driven. This means it's not about the who, but the *what* and the *where*.

As such, data protection is built into the process and specific company policies put in place via the DDR platform. **Think of it this way:** as novel threats are eliminated, Zero Trust DDR also analyzes the content for sensitive data, such as PII, accurately classifying this information on the fly. At this time, it can apply data protections such as masking and anonymization for defined data types while factoring in the context of where the file is going. This real-time process ensures that rebuilt files are free of threats and reduces the accidental sharing of sensitive data with non-approved audiences.

This holistic strategy ensures that all facets of data security, from initial threat detection to ensuring compliance with privacy laws, are managed in a cohesive and integrated manner. By doing so, Zero Trust DDR offers an all-encompassing solution that guards against external threats and fortifies internal data management practices.



Zero Trust DDR

The Technical and Business Benefits

Zero Trust DDR marks a paradigm shift in cybersecurity, offering a robust and comprehensive shield against data breaches and cyber threats. This modern-day approach seamlessly integrates cutting-edge technology with company-specific strategic processes, significantly elevating an organization's defense mechanisms while reducing noise and technological redundancies. Think better posture, less fatigue.

DDR itself stands out in its ability to confront and navigate the complexities of modern cybersecurity challenges, going beyond traditional security measures to align with business objectives and deliver substantial value – both now and into the future. Integrating Zero Trust principles allows DDR to deliver the zero-day protection that organizations in the GenAI era need to prevent the next big data breach.

With Zero Trust DDR, organizations can champion a cohesive defense strategy that merges effortlessly with current security systems, in which organizations have invested **$1.75 trillion globally**.

Let's take a deeper look...

The Technical Benefits of DDR

The primary advantages of Zero Trust DDR lie in its technical capabilities, particularly in advanced threat detection and data protection. Utilizing sophisticated algorithms and machine learning, DDR proactively identifies and neutralizes potential cyber threats before they manifest into damaging incidents. This system is crafted for real-time responsiveness, ensuring immediate action upon detecting security issues.

DDR also protects privacy by analyzing data in motion for sensitive information. It rapidly classifies this data and applies relevant protections such as masking and anonymization. This way, data is seamlessly sanitized of sensitive data without burdening IT, SOCs, or end-users.

Unlike other security solutions, DDR is designed for compatibility and seamless integration with existing security infrastructure. By enhancing and working in tandem with current security systems, DDR adds an extra layer of protection and optimizes the overall effectiveness of existing cybersecurity tools and strategies.

The Business Benefits of DDR

DDR goes beyond its technical application and aligns with core business objectives, such as managing risks and adhering to regulatory standards. This compliance with PCI-DSS, HIPAA, and other regulations both local and international, is critical to protecting organizations from potential legal and financial consequences, significantly enhancing customer trust and bolstering the organization's reputation in the marketplace.

Just as any solution requires an initial investment, DDR's long-term cost-effectiveness cannot be overstated. Its proactive nature in preventing data breaches and further loss saves substantial costs associated with cyber incidents and fortifies the organization's operational integrity. At this point, we'd be remiss not to re-state the fact that breaches cost organizations an **average of $4.45 million** per year. With the right solution in place, this doesn't have to be a number worth worrying about.

Votiro Brings Zero Trust to Data Detection & Response

Today, CISOs, IT personnel, and security vendors have their pick of the litter when it comes to cybersecurity tools, including versions of DDR. However, only one delivers true Zero Trust Content Security + Data Detection & Response in one platform — **Votiro**.

With real-time privacy and compliance, proactive file-borne threat prevention, and actionable data insights, Votiro protects organizations (in any number of industries) around the globe from countless digital threats that pose unnecessary risks to their team, their customers, and their reputation.

Delivering everything you've read about DDR above, Votiro's Zero Trust DDR is designed to unify threat prevention and data privacy without adding more work or more alarms, offering unparalleled business security when and where it's needed most. Not only does Votiro eliminate malware effectively while detecting and protecting sensitive data, it ensures regulatory compliance, a reduced reliance on growing tech stacks, and a more robust security posture.

By adopting a proactive stance and integrating a zero-trust approach, Votiro provides a modern defense mechanism that addresses potential vulnerabilities before they can be exploited.

To learn more about Votiro's Data Detection & Response capabilities, book a **one-on-one platform demo** where our file experts will help you understand your risk surface and where Votiro can plug zero-day vulnerabilities and privacy gaps.

Or t**ry Votiro free for 30 days** and see for yourself how our proactive data security solution defends your endpoints and sensitive data in real-time – without disrupting your productivity.

VOTIRO

We make file-borne threats and privacy risks a thing of the past.

Contact Sales

Visit Website